Supreme Court, U.S
FILED
DEC 15 2003
OFFICE OF THE CLERK

No. 03-5554

IN THE

Supreme Court of the United States

LARRY D. HIIBEL,

Petitioner,

v.

SIXTH JUDICIAL DISTRICT COURT OF NEVADA, HUMBOLDT COUNTY, ET AL.,

Respondent.

BRIEF OF AMICI CURIAE ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND LEGAL SCHOLARS AND TECHNICAL EXPERTS

MARC ROTENBERG
Counsel of Record
DAVID L. SOBEL
MARCIA HOFMANN
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009
(202) 483-1140

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE AMICI CURIAE 1

SUMMARY OF THE ARGUMENT 3

ARGUMENT 5

I. THE NATIONAL CRIME INFORMATION CENTER 6
- A. Establishment of the NCIC 7
- B. Ongoing Concerns About NCIC Record Accuracy 7

II. THE MULTI-STATE ANTI-TERRORISM INFORMATION EXCHANGE (MATRIX) 11
- A. Operation of MATRIX 11
- B. Privacy Concerns Have Led States to Withdraw from MATRIX 14
- C. MATRIX Data Will Be Available to Police Officers on the Street 15

III. DRIVER AND VEHICLE INFORMATION DATABASE (DAVID) 17
- A. DAVID is Readily Accessible to Law Enforcement Agents 20
- B. The DAVID System Raises Substantial Privacy Concerns 20

IV. TRANSPORTATION WORKERS IDENTIFICATION CREDENTIAL (TWIC) 21

V. US-VISIT SYSTEM 23
- A. Operation of US-VISIT System 26
- B. Missing Privacy Impact Assessment 28
- C. Dramatic Expansion of US-VISIT 29

CONCLUSION 30

TABLE OF AUTHORITIES

Cases

Arizona v. Evans, 514 U.S. 1 (1995) 3, 7, 8

Reno v. Condon, 528 U.S. 141 (2000) 21

Sultaan Lakia Myke Freeman v. Florida Dep't of Highway Safety and Motor Vehicles, No. 2002-CA-2828 (Fla. Cir. Ct. June 6, 2003). 20

Terry v. Ohio, 392 U.S. 1 (1968) 4, 9, 10

Whalen v. Roe, 429 U.S. 589 (1977) 5

Statutes

Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-546 (1996) (codified as amended at 8 U.S.C. § 1221 (1996)) 24

Immigration and Naturalization Service Data Management Improvement Act of 2000, Pub. L. No. 106-215, 114 Stat. 337 (2000) (codified as amended at 8 U.S.C. § 1365a (2000)) 24

Visa Waiver Permanent Program Act, Pub. L. No. 106-396, 114 Stat. 1637 (2000) (codified as amended at 8 U.S.C. § 1187 (2002)) 27

Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 272 (2001) (codified as amended at 49 U.S.C. § 44909 (c)(2)(F)(5) (2001)) 28

Electronic Government Act of 2002, Pub. L. No. 107-347, Title II, 116 Stat. 2910 sec. 208 (2002) (codified as amended at 44 U.S.C. § 3601 note (2003)) 28

The Privacy Act, 5 U.S.C. § 552a 9

5 U.S.C. § 552a(e)(1) 9

5 U.S.C. § 552a(e)(5) 9

8 U.S.C. § 1221(c) 26

8 U.S.C. § 1379(3)(C) 28

Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001, 8 U.S.C. § 1635a 24

8 U.S.C. § 1635a(f)(2) 28

8 U.S.C. § 1635a note 28

Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173 (2002) (codified as amended at 8 U.S.C. § 1722 (2002)) 25

8 U.S.C. § 1722(a)(5)(C) 26

8 U.S.C. § 1731(a)(2) 25

8 U.S.C. § 1732 (b)(1) 25

Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 21

28 U.S.C. § 534 6

46 U.S.C. § 70105 21

49 U.S.C. § 114, 44903(g) 21

Fla. Stat. § 119.07(3)(aa) (2002) 21

O.C.G.A. § 40-5-2(c)(1)(D) 15

Administrative Materials

Privacy Act of 1974; Implementation, 68 Fed. Reg. 14140 (March 24, 2003) (codified at 28 C.F.R. pt. 16) 9

Transportation Worker Identification Credentialing (TWIC) System, 68 Fed. Reg. 49496 (Aug. 18, 2003) 21, 22, 23

28 C.F.R. § 16.96(g)(1) 9

Miscellaneous Sources

Press Advisory, Thurbert Baker, Ga. Attorney General, Attorney General Baker Declares Transfer of Driver information to MATRIX Database Illegal (Oct. 20, 2003) *at* http://www.state.ga.us/ago/press/press.cgi?prfile=PR.20031020.01 ..... 12, 14, 15

Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology and Criminal Justice Information*, NCL 187669 (Aug. 2001) *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/rntfptcj.pdf 6

Bureau of Justice Statistics, *Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update*, NCJ 187670 (Dec. 2001), *available at* http://www.ojp.usdoj.gov/bjs/pub/ascii/umchri01.txt 7

..... 7, 8, 9, 10

Criminal and Juvenile Justice Information Systems (CJIS) Council, Minutes of Meeting (Feb. 28, 2003) *at* http://www.fdle.state.fl.us/CJJISCouncil/minutes/FINAL%20minutes%202-28-03.pdf 19

Data Mining: Current Applications and Future Possibilities. Hearing before the House Subcomm. on Tech., Info. Policy, Intergovernmental Relations and the Census, Comm. on Gov't Reform, 108th Cong. (2003) (testimony of Honorable Paula B. Dockery, Fl. State Senator), *at* http://reform.house.gov/UploadedFiles/Dockery.pdf 14, 15, 16, 17

Press Release, Dep't of Homeland Security, DHS Unveils Technology for US-VISIT Entry and Exit Procedures (Oct. 28, 2003) *available at* http://www.useu.be/Categories/Justice%20and%20Home%20Affairs/Oct2803USVISIT.html 27

Press Release, Dep't of Homeland Security, US-VISIT Fact Sheet (Oct. 28, 2003) *available at* http://www.dhs.gov/dhspublic/display?content=20280 ..... 26, 29

Dep't of Homeland Security, *US-VISIT Q&As*, *available at* http://www.dhs.gov/interweb/assetlibrary/USVISIT_QnA_102703.pdf 25, 26, 27

FDLE Commissioner James Moore, Remarks to Fla. Sheriffs Winter Conference (Jan. 26, 2003) *at* http://www.fdle.state.fl.us/publications/speeches/20030126_fl_sheriffs_conf.pdf 11

FDLE Commissioner James Moore, Remarks to Information Processing Interagency Conference (March 4, 2003) *at* http://www.fdle.state.fl.us/publications/speeches/20030304_g

itec.pdf 17

Press Release, Federal Bureau of Investigation (July 15, 1999) *at* http://www.fbi.gov/pressrel/pressrel99/ncic2000.htm 6

Fla. Dep't of Highway Safety and Motor Vehicles, DHSMV Data Warehouse, *at* http://casey.hsmv.state.fl.us/intranet/ddl/AAMVA/warehouse.pdf 18

Fla. Dep't of Highway Safety and Motor Vehicles, DAVID Brochure, *at* http://casey.hsmv.state.fl.us/intranet/ddl/AAMVA/david.pdf 17, 18, 19, 20

Fla. Dep't of Highway Safety and Motor Vehicles, Drivers License Homepage, *at* http://casey.hsmv.state.fl.us/intranet/ddl/AAMVA/aamva.html 17

Fla. Dep't of Law Enforcement, *Successful use of technology to improve public safety: CJNet at* http://www.fdle.state.fl.us/Publications/tech_success_stories/cjnet.htm 18

Fla. Highway Patrol, *Laptop Gives Trooper the Edge, at* http://www.fhp.state.fl.us/html/photogallery/Laptops031103.html 17, 19, 20

General Accounting Office, *Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning*, GAO-03-563 (June 9, 2003) 28

General Accounting Office, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to be Addressed*, GAO-03-1083 (Sept. 2003), *available at* http://www.gao.gov/new.items/d031083.pdf 24, 26

Ariel Hart, *National Briefing: South: Georgia Pulling Out of*

Terror Database, N.Y. Times, Oct. 23, 2003, *available at* http://query.nytimes.com/gst/fullpage.html?res=950DE1D61731F930A15753C1A9659C8B63 . . . . . 14, 15

Lisa Hopkins, FDLE Planning Consultant, General Services Agency, "Florida's Success at Interagency Information Fusion for Domestic Security" *at* http://www.gsa.gov/cm_attachments/GSA_PUBLICATIONS/13-FloridaDomestic_R2C-k56_0Z5RDZ-i34K-pR.htm 13

Institute of Intergovernmental Research, *MATRIX Home*, *at* http://www.iir.com/matrix 16

Institute for Intergovernmental Research, *MATRIX Overview, at* http://www.iir.com/matrix/overview.htm 14, 19

Institute for Intergovernmental Research, *MATRIX Program Objectives #1, at* http://www.iir.com/matrix/objectives_1.htm 13, 16

Institute for Intergovernmental Research, *MATRIX Program Objectives #2*, *at* http://www.iir.com/matrix/objectives_2.htm 12

Institute for Intergovernmental Research, *MATRIX Program Objectives #3, at* http://www.iir.com/matrix/objectives_3.htm 15, 17

Press Release, International Information Programs, U.S. Dep't of State, *New Entry-Exit System for Visitors to U.S. Will Be Fast and Effective* (Oct. 28, 2003) *available at* http://usinfo.state.gov/topical/pol/terror/texts/03102807.htm 29

Vernon Keenan, Director of Ga. Bureau of Investigation, *Safeguards Prevent Abuse of MATRIX*, Atlanta Journal-

Constitution, Oct. 16, 2003, *available at* http://www.ajc.com/opinion/content/opinion/1003/ 16

Susan Lambert, Director, Fla. Division of Drivers Licenses, Connecting the Dots...with Integrated Services, Presentation to American Association of Motor Vehicle Administrators *at* http://casey.hsmv.state.fl.us/intranet/ddl/AAMVA/AAMVAconf003ppt2000.ppt 18, 19, 20

MATRIX and ATIX: Information Programs Developed in Response to September 11, 2001, Ga. Homeland Security Bulletin No. 20-03 (Ga. ~~Office~~ of Homeland Security), Aug. 1, 2003, *at* http://www.gahomelandsecurity.com/bulletins/2003/August%2003/20-03%20August%201.pdf 12, 13, 14, 15, 16

Robert O'Harrow, Jr., *U.S. Backs Florida's New Counterterrorism Database,* Wash. Post, Aug. 6, 2003. at A1 14

Press Release, SeisInt, Inc., AccurInt Arms Law Enforcement (undated) *at* http://www.accurint.com/images/law.pdf 13, 14

Press Release, Ga. Governor Sonny Perdue, Statement of Governor Perdue Regarding the MATRIX Database (Oct. 21, 2003) *at* http://www.gov.state.ga.us/document.asp?doc=press/press279 15

Security Credentials for Port Personnel Before the House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation, 107th Cong. (Feb. 13, 2002) (statement of Rear Admiral James Underwood) 22

Press Release, SeisInt, Inc., AccurInt Arms Law Enforcement, *at* http://www.accurint.com/images/law.pdf 13

Press Release, Senate Committee on Governmental Affairs, DHS Violates Privacy Impact Requirements with US VISIT Technology (Dec. 4, 2003), *available at* http://www.senate.gov/~gov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=599&Month=12&Year=2003 29

Transportation Safety Administration, *Transportation Worker Identification Credential (TWIC) Stakeholder Brief* (July 2003) 21, 22, 23

Letter from Fla. Dep't of Law Enforcement Commissioner Guy Tunnel to Fla. Today Editorial Editor John Glisch (Oct. 30, 2003) *available at* http://www.fdle.state.fl.us/osi/DomesticSecurity/1103/MATRIX.htm 11

INTEREST OF THE AMICI CURIAE [1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. that was established in 19994 to focus public attention on emerging civil liberties issues. EPIC has participated as *amicus curiae* in numerous privacy cases, including *Doe v. Chao*, No. 02-1377 (2003), *Smith v. Doe*, 123 S. Ct. 1140 (2003), *Dep't. of Justice v. City of Chicago*, 123 S. Ct. 1352 (2003), *Watchtower Bible and Tract Soc'y of N.Y. Inc. v. Vill. of Stratton*, 536 U.S. 150 (2002), and *Reno v. Condon*, 528 U.S. 141 (2000).

Amici Legal Scholars and Technical Experts

Ann Bartow, Assistant Professor of Law, University of South Carolina School of Law

James Boyle, William Neal Reynolds Professor of Law, Duke University Law School

Oscar Gandy, Professor, Annenberg School of Communications

Jerry Kang, Visiting Professor of Law, Harvard Law School

Dr. Peter G. Neumann, Principal Scientist, SRI International Computer Science Laboratory

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. In accordance with Rule 37.6 it is stated that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party. Law school students participating in the EPIC Internet Public Interest Opportunities Program (IPIOP) Munged Dolah, Tiffany A. Stedman, and Michael Trinh assisted in the preparation of the brief.

Pamela Samuelson, Chancellor's Professor of Law and Information Management, University of California, Berkeley

Dr. Bruce Schneier, Chief Technical Office, Counterpaine Internet Security

Dr. Barbara Simons, Former President, Association for Computing Machinery

Robert Ellis Smith, Publisher, *Privacy Journal*

Daniel J. Solove, Visiting Associate Professor, George Washington University School of Law

(affiliations are for identification only)

SUMMARY OF THE ARGUMENT

A name is now no longer a simple identifier: it is the key to a vast, cross-referenced system of public and private databases, which lay bare the most intimate features of an individual's life. If any person can be coerced by the state to hand over this key to the police, then the protections of the Fourth and Fifth Amendments have been rendered illusory.

The compelled disclosure of personal identification is central to the Court's consideration of this case. Critical to understanding the full consequences of providing identifying information to the police in the modern era is a close examination of the government databases and legal authority that now exists in the United States. Today the police have the ability to peruse increasingly sophisticated computer databases containing information wholly unrelated to the reason for an initial police stop.

Information systems that are currently available to the police, or may soon become available, include the National Crime Information Center ("NCIC"), the Multi-State Anti-Terrorism Information Exchange ("MATRIX"), the United States Visitor and Immigrant Status Indicator Technology System ("US-VISIT"), the Driver And Vehicle Information Database ("DAVID"), and the Transportation Workers Identification Credential ("TWIC").

Routine police access to these systems present a range of potential problems. Specifically, the record inaccuracies in the NCIC have been further compounded by the recent decision of the Department of Justice to exempt the record system from the data quality requirements of the Privacy Act, even after the Court's opinion in *Arizona v. Evans*, 514 U.S. 1 (1995), which raised concern about police reliance on faulty data systems.

The MATRIX system raises such troubling privacy concerns, for example, by integrating information from private sector and public sector record systems apparently without regard to the application of state privacy law, that several of the original state partners have withdrawn from the multi-state network project.

US-VISIT, a system of biometric identification originally intended for use by border control officials at ports of entry to the United States, will now enable law enforcement officers routinely to identify individuals, including students on university campuses, within the country.

DAVID, a record system built on motor vehicle information, gives the police rapid access to information that is subject to state and federal privacy law. The DAVID system is evolving rapidly from a government database intended to enforce motor vehicle laws to a general purpose system of identification that could be used routinely in police stops.

Finally, TWIC is an elaborate identification system that will provide police an extensive database of information about individuals who work in the transportation sector.

These systems raise significant Fourth Amendment and Fifth Amendment concerns and implicate individual liberty. The compelled production of personal identification now permits the government to engage in a far more extensive search of personal information stored in government databases than was ever contemplated in *Terry* v. *Ohio*, 392 U.S. 1 (1968). Further, the mere fact of a police stop may now create a transaction record that will be stored in government record systems, regardless of whether an arrest occurs. While it may be appropriate in the context of a lawful stop of a motor vehicle for the police to determine whether the vehicle is lost or stolen or whether there are

outstanding warrants for the driver, it would not be appropriate for the police to conduct such a search of an individual prior to an arrest.

It should be anticipated that the police will obtain ever more efficient systems to monitor and track individuals through interconnected databases. The Supreme Court has repeatedly cautioned that there may come a time when clear safeguards, rooted in the Fourth and Fifth Amendments, on the use of such systems should be established. *See, e.g., Whalen v. Roe*, 429 U.S. 589, 607 (1977) (Brennan, J., concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, . . ."). That time has now come.

Given the extraordinary scope and capability of these new systems, which could easily become systems of mass public surveillance, *amici* believe it is critical for the Court to oppose the coerced disclosure of identity and to ensure that the police do not use a *Terry* stop for an unbounded fishing expedition of government computer databases.

ARGUMENT

Police officers today have access to an extraordinary range of detailed personal information in government databases that could easily give rise to further investigations unrelated to the reasons for the initial detention. Moreover, much of the information contained in these databases is often inaccurate and unreliable. Some of the information is obtained from private record systems and was never intended to be used for law enforcement purposes.

In this context, the compelled disclosure of actual identity in circumstances where probable cause to arrest is lacking raises significant Constitution concerns. The scope and problems associated with the government record systems described below underscore the need for the Court to ensure

that an investigatory stop not become the basis for an extensive fishing expedition across government databases.

I. The National Crime Information Center

The National Crime Information Center ("NCIC") is a system that makes criminal history information widely available to police officers and law enforcement officials across the United States. *See generally* Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology and Criminal Justice Information*, NCL 187669, at 47 (Aug. 2001);[2] *see also* Press Release, Federal Bureau of Investigation (July 15, 1999).[3]

The Attorney General has the authority to "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records" and "exchange such records and information with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions." 28 U.S.C. § 534 (2002). Furthermore, information can be entered into the system by either federal or state authorities. *Id.* A non-exhaustive list of information that Congress envisioned the NCIC to contain includes "arrests, convictions, and arrest warrants for stalking or domestic violence or for violations of protection orders for the protection of parties from stalking or domestic violence; and protection orders for the protection of persons from stalking or domestic violence, provided such orders are subject to periodic verification." *Id.*

[2] *Available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/rntfptcj.pdf (last visited Nov. 24, 2003).

[3] *Available at* http://www.fbi.gov/pressrel/pressrel99/ncic2000.htm (last visited Nov. 24, 2003).

A. Establishment of the NCIC

The FBI established the predecessor to the NCIC in 1967 "to provide a nationwide, user-orientated computer response for criminal justice records." Bureau of Justice Statistics, *Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update*, NCJ 187670 at 26 (Dec. 2001) [hereinafter "BJS Report"].[4] Today the NCIC is the most extensive criminal history record systems in the United States. "[M]ore than 59 million individual offenders were in the criminal history files of the State central repositories as of December 31, 1999." *Id.* at 30. "At the Federal level, the FBI's Criminal Justice Information Services ("CJIS") Division maintains automated, fingerprint-based criminal history record information with respect to more than 43 million individuals in [the Interstate Identification Index]." *Id.* at 31.

Identification information available typically includes an individual's name, address, date of birth, Social Security Number, sex, race and physical characteristics. *Id.* at 28-29. These databases may also include an individual's place of employment, automobile registration, fingerprints, criminal history information, and juvenile record information, among other identifiers. *Id.* However, the BJS Report cautions that "name searches are not fully reliable and existing criminal record files may be inaccurate and incomplete, particularly with respect to case disposition information." *Id.* at 21.

B. Ongoing Concerns About NCIC Record Accuracy

In 1995, the Court upheld the use of evidence obtained from an erroneous arrest record (the product of a clerical error), but Justice O'Connor wrote separately to

[4] A*vailable at* http://www.ojp.usdoj.gov/bjs/pub/ascii/umchri01.txt (last visited Nov. 24, 2003).

express concern about reliance on error-prone recordkeeping systems. *Arizona v. Evans*, 514 U.S. 1, 16-17 (1995) (O'Connor, J., concurring). Justice O'Connor explained:

> [w]hile the police were innocent of the court employee's mistake, they may or may not have acted reasonably in their reliance *on the recordkeeping system itself*. Surely it would *not* be reasonable for the police to rely, say, on a recordkeeping system, their own or some other agency's, that has no mechanism to ensure its accuracy over time and that routinely leads to false arrests, even years after the probable cause for any such arrest has ceased to exist (if it ever existed).

Id. at 17 (emphasis in original).

Nonetheless, the recent Bureau of Justice Statistics report identifies ongoing concerns about the accuracy and reliability of NICIC records. According to the BJS report, "inadequacies in the accuracy and completeness of criminal history records is *the single most serious deficiency* affecting the Nation's criminal history record information system." BJS Report at 38 (emphasis added). Moreover, if incomplete or inaccurate records are used "there is a substantial risk that the user will make an incorrect or misguided decision." *Id.* Because the criminal history information is available to both private and public entities, misguided decisions may lead to an unjustified arrest, a lost employment opportunity, or inability to purchase a firearm. *Id.*

There have not been many "in-depth audits or reviews of the accuracy of the information maintained by State and Federal criminal history record repositories" conducted, according to the report, but "most of those that have been conducted have found unacceptable levels of inaccuracies." *Id.* at 39.

The problem of NCIC record accuracy has been compounded by recent actions of the Department of Justice. In March 2003, the Justice Department exempted the NCIC from numerous mandates established by the Privacy Act, 5 U.S.C. § 552a, most notably accuracy requirements. Privacy Act of 1974; Implementation, 68 Fed. Reg. 14140 (March 24, 2003) (codified at 28 C.F.R. pt. 16). As a result of this exemption, the FBI need not comply with 5 U.S.C. § 552a(e)(5), which requires an agency to "maintain all records which are used by the agency in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual[.]" 28 C.F.R. § 16.96(g)(1). The NCIC is also exempt from 5 U.S.C. § 552a(e)(1), which requires that a system of records contain "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency[.]" *Id.*

On the state level, the types and completeness of records included in the NCIC vary significantly depending on each state's resources. BJS Report at 31. The BJS Report finds that "there is still substantial variation among disposition reporting requirements." *Id.* at 35. For example, "[t]hirty-two States require law enforcement agencies to notify the State central repository when an arrest person is released without formal charging after fingerprints have been sent to the repository, while 19 jurisdictions have no such requirement." *Id.* In the thirty-two states that recorded such information, up to 40 percent of arrests within the five years preceding the BJS Report did not list the final dispositions. *Id.* at 38.

This inconsistency may cause certain non-reporting state systems to reflect an arrest that may have been unjustified, with no indication of the result. The false report of an arrest is important because, as the Court emphasized in

Terry, "[a]n arrest is a wholly different kind of intrusion upon individual freedom from a limited search for weapons" because "[a]n arrest is the initial stage of a criminal prosecution . . . and it is inevitably accompanied by future interference with the individual's freedom of movement, whether or not trial or conviction ultimately follows." 392 U.S. 1, 26 (1968).

Duplicate records are also a problem, as are diverse formats and differences in content. BJS Report at 39, 41. Duplicate records stem from false names and clerical errors, while differences in content and format are a result of varying technological and legal schemes that the various states have adopted. *Id.*

The NCIC operates a private telecommunications system throughout the nation. *Id.* at 27. The FBI receives input for the system from "criminal justice agencies at every level of government—Federal, State, and local—and at each stage of the criminal justice system—by police departments, prosecutors, courts, and corrections agencies." *Id.* at 32. Efforts are underway to create a "nationwide telecommunications system that will permit the electronic exchange of criminal history information and related graphics throughout the country in a paper-free 'lights out' environment." *Id.* at 33. While online access to NCIC information varies by jurisdiction, terminals can either be in a centralized location, such as the police station house, or in moveable locations, such as police cars. *Id.* at 36.

As a result, police officers across the country have routine access to the NCIC, but the ongoing concerns about data quality, coupled with the extensive records that are made available, mean that a routine query to the NCIC could produce inaccurate information or information unrelated to the reason for the stop.

II. The Multi-State Anti-Terrorism Information Exchange (MATRIX)

The Multi-State Anti-Terrorism Information Exchange ("MATRIX") is a state-run database system intended to allow law enforcement agencies in participating states to analyze information from multiple criminal and public record sources in near-real time, through a single web-based query. It is an example of the type of record system that seeks to link together a wide range of public and private record systems that will then be made available to law enforcement agents in the field. So little attention has been given to privacy concerns that several of the original state partners recently have withdrawn from the MATRIX project.

MATRIX uses a data mining system called "Factual Data Analysis" to analyze public and private data sources. MATRIX was developed by the Florida Department of Law Enforcement ("FDLE") and a private company, SeisInt, Inc., and is already utilized by 1,000 law enforcement agency users in Florida. Letter from Fla. Dep't of Law Enforcement Commissioner Guy Tunnel to Fla. Today Editorial Editor John Glisch (Oct. 30, 2003).[5]

FDLE Commissioner James Moore has hailed MATRIX as the first step in developing "a national (not federally controlled) intelligence network." FDLE Commissioner James Moore, Remarks to Fla. Sheriffs Winter Conference (Jan. 26, 2003).[6]

A. Operation of MATRIX

MATRIX is implemented over a criminal justice network, the Regional Information Sharing System Network

---

[5] *Available at* http://www.fdle.state.fl.us/osi/DomesticSecurity1103/ MATRIX.htm (last visited Nov. 24, 2003).

[6] *Available at* http://www.fdle.state.fl.us/publications/speeches/20030126_fl_sheriffs_conf.pdf (last visited Nov. 24, 2003).

("RISSNET"). RISSNET connects 5,700 law enforcement agencies in fifty states and the District of Columbia. *MATRIX and ATIX: Information Programs Developed in Response to September 11, 2001*, Ga. Homeland Security Bulletin No. 20-03 (Ga. Office of Homeland Security), Aug. 1, 2003 at 1[7]; Institute for Intergovernmental Research, *MATRIX Program Objectives #2*.[8] MATRIX will provide access to other web-enabled "document storage systems" similar to those found on RISSNET. *Id.*

MATRIX is operated by a private company, SeisInt, Inc. The personal data is stored on computers owned and operated by SeisInt. This has raised significant concerns about compliance with state privacy laws. *See, e.g.*, Press Advisory, Thurbert Baker, Ga. Attorney General, Attorney General Baker Declares Transfer of Driver information to MATRIX Database Illegal (Oct. 20, 2003).[9]

The MATRIX database includes personal information obtained from public information and private databases. The combined database provides access to an extraordinary range of personal information. Available documentation indicates that the MATRIX system currently includes:

1. Criminal history
2. Driver license information
3. Vehicle registration
4. Incarceration/corrections records
5. Digitized photographs

[7] *Available at* http://www.gahomelandsecurity.com/bulletins/2003/August%2003/20-03%20August%201.pdf (last visited Nov. 24, 2003).

[8] *Available at* http://www.iir.com/matrix/objectives_2.htm (last visited Nov. 24, 2003).

[9] *Available at* http://www.state.ga.us/ago/press/press.cgi?prfile=PR.20031020.01 (last visited Nov. 24, 2003).

6. Investigative data
7. Property ownership
8. Address history
9. Marine vessel registration
10. U.S. directory assistance
11. Public utility service connections
12. Bankruptcies
13. Liens and judgments
14. UCC filings
15. U.S. domain names
16. Concealed weapons permits
17. DEA controlled substances licenses
18. FAA aircraft and pilots licenses
19. Federal firearms and explosives licenses
20. Hunting and fishing licenses
21. Professional licenses
22. Voter registration

Ga. Office of Homeland Security, *supra;* Institute for Intergovernmental Research, *MATRIX Program Objectives #1; see* Press Release, SeisInt, Inc., AccurInt Arms Law Enforcement.[10]

MATRIX also includes searchable image data. These digitized images are associated with personal information. FDLE Planning Consultant Hopkins, *supra*. MATRIX image data include visual mapping data and individuals' pictures. MATRIX can generate "photo 'line-ups'" from an investigative query. Ga. Office of Homeland Security, *supra*. MATRIX may also be used for visual mapping, which means that an investigator would find a list of all persons who had lived at a requested address. *Id.*

MATRIX is funded partially by the Department of Justice, Office of Justice Programs, Bureau of Justice

[10] *Available at* http://www.accurint.com/images/law.pdf (last visited Nov. 24, 2003).

Assistance through a $4 million grant. *Data Mining: Current Applications and Future Possibilities. Hearing before the House Subcomm. on Tech., Info. Policy, Intergovernmental Relations and the Census, Comm. on Gov't Reform,* 108th Cong. (2003) (testimony of Hon. Paula B. Dockery, Fla. State Senator) at 5.[11] The grant to the Florida-led state consortium was for database integration, hardware, software, and network support. Institute of Intergovernmental Research, *MATRIX Overview.*[12] The Department of Homeland Security has pledged a further $8 million towards the project. Robert O'Harrow, Jr., *U.S. Backs Florida's New Counterterrorism Database: 'Matrix' Offers Law Agencies Faster Access to Americans' Personal Records,* Wash. Post, Aug. 6, 2003, at A1 ("Police in Florida are creating a counterterrorism database designed to give law enforcement agencies around the country a powerful new tool to analyze billions of records about both criminals and ordinary Americans.")

B. Privacy Concerns Have Led States to Withdraw from MATRIX

Thirteen states originally agreed to participate in MATRIX: Alabama, Connecticut, Florida, Georgia, Kentucky, Louisiana, Michigan, New York, Oregon, Pennsylvania, South Carolina, Ohio, and Utah. Ga. Office of Homeland Security, *supra*; *see* Fla. State Senator Dockery, *supra at* 5. Six states (Alabama, Georgia, Kentucky, Louisiana, Oregon, South Carolina) have dropped out citing a variety of privacy and budget concerns. Ariel Hart, *National Briefing: South: Georgia Pulling Out of Terror Database,*

[11] *Available at* http://reform.house.gov/UploadedFiles/Dockery.pdf (last visited Nov. 24, 2003).

[12] *Available at* http://www.iir.com/matrix/overview.htm (last visited Nov. 24, 2003).

N.Y. Times, Oct. 23, 2003, at A26;[13] *see also* Press Release, Ga. Governor Sonny Perdue, Statement of Governor Perdue Regarding the MATRIX Database (Oct. 21, 2003).[14]

Georgia has ceased participation in MATRIX specifically because of privacy concerns over compliance with state privacy laws. Ga. Att'y Gen. Baker, *supra*. Georgia Attorney General Thurbert Baker found that regular transfer of Georgia driver information to FDLE would violate Georgia state laws limiting transfer of data in the driver information database. *Id.* Under Georgia state law, driving records may be transferred only in response to a specific allegation of criminal conduct or unlawful activity. *Id* (applying O.C.G.A. § 40-5-2(c)(1)(D)). In a public statement ending Georgia's participation in MATRIX, Governor Sonny Perdue also expressed "serious concerns about the privacy interests involved" and withheld further transfer, even if lawful, of any state records to MATRIX. Ga. Governor Perdue, *supra*; *see also* Ga. Att'y Gen. Baker, *supra*.

C. MATRIX Data Will Be Available to Police Officers on the Street

According to the planning documents, MATRIX will provide a "mechanism for local officers to share important information they collect 'on the street' with other law enforcement agencies." Institute for Intergovernmental Research, *MATRIX Program Objectives #3.*[15] The Georgia Homeland Security Bulletin describes the MATRIX as being

[13] *Available at* http://query.nytimes.com/gst/fullpage.html?res=950DE1D61731F930A15753C1A9659C8B63 (last visited Dec. 12, 2003).

[14] *Available at* http://www.gov.state.ga.us/document.asp?doc=press/press279 (last visited on Nov. 24, 2003).

[15] *Available at* http://www.iir.com/matrix/objectives_3.htm (last visited Nov. 24, 2003).

able to identify and locate persons "with minimal input and the push of a button." Ga. Office of Homeland Security, *supra*. Further, "investigative queries and analyses may be done in 'real time,'" and "requests that previously took hours, days or week [sic] now take seconds." Ga. Office of Homeland Security, *supra*; *see* Fla. State Senator Dockery, *supra* at 5; Ga. Bureau of Investigation Director Keenan, *supra*. *See generally* Institute of Intergovernmental Research, *MATRIX Home*.[16] Further, the Georgia Homeland Security Bulletin states that use of the MATRIX system in Florida provided "breakthroughs at speeds that otherwise would not have been possible." Ga. Office of Homeland Security, *supra*.

Officials explain that MATRIX is not a surveillance system, and safeguards exist to protect privacy. But there is no probable cause requirement in the FDLE Guidelines for use of MATRIX. FDLE Guidelines require only reasonable suspicion for releasing analyzed data for investigation. *Id*. at 3. Moreover, reasonable suspicion is not required for the MATRIX system to analyze data internally, since some analysis processes run automatically. *Id*. at 4. In applying the "Factual Data Analysis" component of MATRIX towards terrorist investigation, Florida uses private data mining entities to analyze public data records using law enforcement-defined criteria to produce a "probability score for criminal behavior." Fla. State Senator Dockery, *supra* at 4. These scores direct law enforcement officials to "locate, target, and monitor" subjects. *Id*. at 4. The same process is used by the FDLE Financial Crime Analysis Center to analyze data to

[16] *Available at* http://www.iir.com/matrix (last visited Nov. 24, 2003); *see also* SeisInt, Inc. *at* http://www.accurint.com/images/law.pdf (last visited Nov. 24, 2003).

identify suspicious financial activity for further investigation. *Id*. at 3.

Web sites are being developed to disseminate MATRIX data to law enforcement agencies and local officers. FDLE Commissioner James Moore, Remarks to Information Processing Interagency Conference (March 4, 2003);[17] *MATRIX Program Objectives #3*.

III. Driver and Vehicle Information Database (DAVID)

The Driver and Vehicle Information Database ("DAVID") is an integrated database that provides law enforcement access to driver information based on name or vehicle information to Florida criminal justice officers, available over common web browsers. DAVID can be accessed by officers in patrol cars through mobile data terminals, and is used in traffic stops. *See* Fla. Highway Patrol, *Laptop Gives Trooper the Edge* (trooper accessed DAVID through Mobile Data Terminal during traffic stop).[18] DAVID contains descriptive and statistical vehicle data, as well as historical driver license data. Fla. Dep't of Highway Safety and Motor Vehicles, DAVID Brochure [hereinafter "DAVID Brochure"];[19] *see* Fla. Dep't of Highway Safety and Motor Vehicles, Dr ers License Homepage.[20] It is capable of retrieving driver records based on name, tag number, or VIN number. DAVID may further retrieve records from partial, fragmented information of each type. DAVID Brochure.

[17] *Available at* http://www.fdle.state.fl.us/publications/speeches/20030304_gitec.pdf (last visited Nov. 24, 2003).

[18] *Available at* http://www.fhp.state.fl.us/html/photogallery/Laptops031103.html (last visited Nov. 25, 2003).

[19] *Available at* http://casey.hsmv.state.fl.us/intranet/ddl/AAMVA/david.pdf (last visited Nov. 23, 2003).

[20] *Available at* http://casey.hsmv.state.fl.us/intranet/ddl/AAMVA/aamva.html (last visited Nov. 23, 2003).

The Florida Department of Highway Safety and Motor Vehicles ("FDHSMV") has stated that the goal of DAVID is to develop the driver's license information database into a "multi-engine analytical engine" for "integrated homeland security, public safety, intelligence gathering, and investigations." *See* Fla. Dep't of Highway Safety and Motor Vehicles, DHSMV Data Warehouse.[21] Currently, the data within DAVID is already shared with the Florida Department of Law Enforcement ("FDLE"). *Id.*; Susan Lambert, Director, Fla. Division of Drivers Licenses, Connecting the Dots with Integrated Services, Presentation to American Association of Motor Vehicle Administrators 19 [hereinafter "Connecting the Dots Presentation"].[22] FDHSMV provides FDLE with daily updates and a list of non-citizens with false identification. *Id.* at 21.

The FDHSMV is planning to share DAVID information with a variety of criminal justice entities and non-criminal justice entities, *e.g.*, Florida County Tax Collectors, Florida County Sheriffs, Supervisors of Elections, Department of Agriculture and Consumer Services, Department of Education, Department of Revenue, Department of Financial Services. *Id.* at 20.

DAVID is accessible via CJNet, a private data network comprising criminal justice agencies. Fla. Dep't of Law Enforcement, *Successful use of technology to improve public safety: CJNet;*[23] *see* DAVID Brochure. CJNet is itself based on an older private criminal justice network, the Florida Criminal Information Center (FCIC) network, and

[21] *Available at* http://casey.hsmv.state.fl.us/intranet/ddl/AAMVA/warehouse.pdf (last visited Nov. 23, 2003).

[22] *Available at* http://casey.hsmv.state.fl.us/intranet/ddl/AAMVA/AAMVAconf2003ppt2000.ppt (last visited Nov. 23, 2003).

[23] *Available at* http://www.fdle.state.fl.us/Publications/tech_success_ stories/cjnet.htm (last visited Nov. 23, 2003).

run by the FDLE. The FDLE, which runs CJNet, is the same Florida agency that oversees the MATRIX system. *See* Institute of Intergovernmental Research, *MATRIX Overview*. CJNet is also the infrastructure by which the MATRIX system is made available to Florida criminal justice agencies. Criminal and Juvenile Justice Information Systems (CJIS) Council, Minutes of Meeting at 6 (Feb. 28, 2003), (unanimous vote supporting pilot project linking CJNet and MATRIX backbone).[24] It connects to RISSNet, a national, federally funded criminal justice information network. In this manner, data within CJNet (including DAVID) is made available as another data source that would be searchable through a single query to the MATRIX system. *See id.*

DAVID contains current and historical data for any driver's license. It contains the current status of a particular driver's license, current picture, current demographics, current address, and any conditional messages (*e.g.*, "sex offender") attached. DAVID Brochure; Connecting the Dots Presentation at 15. Historical data of the drivers' license is also available, including past histories of personal information, renewal, restrictions, endorsements, and complete driving history. *Id.*

DAVID also retains historical photo data from past image captures, meaning "DAVID maintains photographic evidence of what a person looks like over a broad span of time." DAVID Brochure; Connecting the Dots Presentation at 12. DAVID also stores any foreign ID documents used in applying for a driver's license or ID card. DAVID Brochure; Connecting the Dots Presentation at 14. Foreign nationals applying for temporary driving permits in Florida are required to have their passports scanned into DAVID.

[24] *Available at* http://www.fdle.state.fl.us/CJJISCouncil/minutes/FINAL%20minutes%202-28-03.pdf (last visited Nov. 23, 2003).

Freeman v. Florida Dep't of Highway Safety and Motor Vehicles, No. 2002-CA-2828 at 12 n.9 (Fla. Cir. Ct. June 6, 2003).

A. DAVID is Readily Accessible to Law Enforcement Agents

DAVID requests can be made from a mobile data terminal installed in patrol cars. *See Laptop Gives Trooper the Edge, supra* (trooper accessed DAVID through mobile data terminal during traffic stop). DAVID allows criminal justice officers to access personal information based on only a name, personal information, a tag number, or a Vehicle Identification Number. Connecting the Dots Presentation at 5. Specifically, DAVID allows a user to search for a person's information based on name, Florida driver's license number, foreign document type, Social Security number, vehicle license tag number, Vehicle Identification Number (VIN), or fragmented data. Connecting the Dots Presentation at 5-7; *see* DAVID Brochure; *Laptop Gives Trooper the Edge, supra.*

DAVID allows law enforcement agents in the field to see all related documents for a particular search. For example, when searching for a vehicle record, a user is able to view the personal information of each driver associated with it, and vice versa. Connecting the Dots Presentation at 15. Further, a search for an individual discloses all cars associated with him, and provide access to the personal information of any other persons associated with those cars. *Id.*

B. The DAVID System Raises Substantial Privacy Concerns

DAVID makes extensive use of motor vehicle records, including personal information. This is information that is subject to federal and state and privacy law. *See*

Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725; Fla. Stat. § 119.07(3)(aa) (2002). The Court expressly upheld the Driver's Privacy Protection Act in response to a challenge brought on federalism grounds. *Reno v. Condon*, 528 U.S. 141 (2000). Now it appears that the state of Florida will make this information available in real time to law enforcement officers on the street. Given the range of government agencies that may soon have access to DAVID, there is every reason to believe that law enforcement officers will access the DAVID system during routine steps of individuals unrelated to violations of motor vehicle laws.

IV. Transportation Workers Identification Credential (TWIC)

Government access to personal information in the context of a police stop will also be facilitated by the recent establishment of new systems of identification, such as the Transportation Workers Identification Credential ("TWIC"). TWIC was established run by the Transportation Security Administration ("TSA"). Aviation and Transportation Security Act of 2001, 49 U.S.C. § 114, 44903(g); Maritime Transportation Security Act, 46 U.S.C. § 70105; Transportation Worker Identification Credentialing (TWIC) System, 68 Fed. Reg. 49496, 49508 (Aug. 18, 2003); Transportation Safety Administration, *Transportation Worker Identification Credential (TWIC) Stakeholder Brief* at 3 (July 2003) (on file with EPIC) [hereinafter "TWIC Stakeholder Brief"].

TWIC is an identification card that is issued to transportation workers, authorized visitors, and all other persons requiring unescorted access to transportation infrastructure secure areas. 68 Fed. Reg. at 49508. Those seeking access to certain areas of airports, rail facilities, port facilities, port headquarters, and pipelines will require the

TWIC card to enter. A central TWIC database, run by TSA, stores personal information and validate a person's eligibility to enter these areas. TWIC Stakeholder Brief, *supra*. The central TWIC database will also run background checks and check a person's identity against other national "watch list" threat-intelligence databases. *Security Credentials for Port Personnel Before the House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation*, 107th Cong. (Feb. 13, 2002) (statement of Rear Admiral James Underwood); TWIC Stakeholder Brief, *supra*, at 10-11. Persons required to have TWIC identification cards will include foreign merchant mariners and foreign truck drivers. *Id*. TWIC stores data on an identification card carried by each transportation employee. *Id*.

These cards are required for entry through Access Control Points, which grant access to certain areas by matching the data stored on the card with data stored at the central TSA data center. *Id*. Access Control Points include vehicle gates, truck lanes, personnel turnstiles, building doors, and pedestrian entrances. *Id*.

The pilot project implementation of the TWIC database contains the following data elements:

Name
Address
Phone Number
Social Security Number
Date of Birth
Place of Birth
Administrative Identification Code
Unique Card Serial Number
Systems Identification Code
Company/Organization Affiliation
Issue Date
Biometric data

Photographic data
Access Level Information
Expiration Date

68 Fed. Reg. at 49508.

This data is stored at Regional Database and Issuance centers and a centralized TSA data center. TWIC Stakeholder Brief, *supra*, at 10-11. The central TSA data center matches individuals against persons appearing in national "watch list" database, and revokes access to all TWIC facilities from such persons. *Id*. at 12.

It is clearly anticipated that the TWIC record system will be made available to police officers on the street.[25] Moreover, the TWIC identification card, since it will be widely used by individuals in the transportation industry, could easily be the document that police would request in routine stops.

V. US-VISIT System

The most elaborate system of identification in the United States is currently being developed by the Department of Homeland Security ("DHS"). The United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") is an integrated government-wide program intended to improve

---

[25] According to the federal regulations, data within the TWIC database will be made available to "the appropriate Federal, State, local, . . . foreign, or international agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where TSA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation . . . a Federal, State, local, . . . foreign, or international agency, where such agency has requested information relevant or necessary for the hiring or retention of an individual as an employee or a contractor . . . [and] international and foreign governmental authorities in accordance with law and formal or informal international agreement . . . " 68 Fed. Reg. at 49508.

the nation's capacity for collecting information on foreign nationals who travel to the United States, as well as control the pre-entry, entry, status, and exit of these travelers. General Accounting Office, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to be Addressed,* GAO-03-1083 (Sept. 2003) at 1.[26]

Congress initially directed the Attorney General to develop an automated entry and exit control system to collect records of arrival and departure from every foreign visitor entering and leaving the United States in Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 ("IIRIRA"). Pub. L. No. 104-208, 110 Stat. 3009-546 (1996) (codified as amended at 8 U.S.C. § 1221 (1996)). Congress later amended and replaced Section 110 of IIRIRA with the Immigration and Naturalization Service Data Management Improvement Act ("DMIA") of 2000. Pub. L. No. 106-215, 114 Stat. 337 (2000) (codified as amended at 8 U.S.C. § 1365a (2000)). The DMIA directed the integration of existing Department of Justice and Department of State electronic foreign visitor arrival and departure databases, including those created at ports of entry and at consular offices. 8 U.S.C. § 1635a(b)(2).

The Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") and the Enhanced Border Security and Visa Entry Reform Act have significantly expanded the operation of the US-VISIT system. In the USA PATRIOT Act, Congress imposed a requirement for "speed" in the program's implementation and mandated that the DHS be consulted with respect to the establishment of the integrated entry and exit program. 8 U.S.C. § 1635a. The

[26] *Available at* http://www.gao.gov/new.items/d031083.pdf (last visited Nov. 24, 2003).

USA PATRIOT Act introduced the concept of biometrics to establish a technology standard that would be used in the development of the US-VISIT the System. Dep't of Homeland Security, *US-VISIT Q&As: Background Information.*[27]

The Enhanced Border Security Act ("EBSA") seeks to fully integrate all databases and data systems maintained by the Immigration and Naturalization Service that process or contain information on aliens. Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173 (2002) (codified as amended at 8 U.S.C. § 1722 (2002)). The EBSA expanded on the USA PATRIOT Act and the DMIA by increasing requirements for US-VISIT's integration, interoperability with other law enforcement and intelligence systems, biometrics, and accessibility. *See* Dep't of Homeland Security, *US-VISIT Q&As: Background Information*, footnote 6. Here Congress specifically mandated the establishment of a database containing the arrival and departure data from machine-readable visas, passports, and other travel and entry documents possessed by aliens. 8 U.S.C. § 1731(a)(2). By October 26, 2004, these travel and entry documents are also to include the use of biometric identifiers in accordance with domestic and international standards organizations. 8 U.S.C. § 1732(b)(1). The EBSA further required all carriers to transmit electronically the information of all visitors and crewmembers arriving and departing the United States by January 1, 2003. Furthermore, the information from the data systems the EBSA describes is to be readily available and easily accessible to any federal law enforcement or intelligence officer responsible for "the

[27] A*vailable at* http://www.dhs.gov/interweb/assetlibrary/USVISIT_QnA_102703.pdf (last visited Nov. 24, 2003).

investigation or identification of aliens." 8 U.S.C. § 1722(a)(5)(C).

A. Operation of US-VISIT System

Along with integrating various databases containing visitor information, US-VISIT will also scan, collect and use biometric identifiers such as fingerprints along with a digital photograph of the visitor. An inkless fingerprinting system will be used upon entry as U.S. Customs and Border Protection Officers review travel documents at Ports of Entry ("POEs"). As both of the visitor's index fingerprints are captured, a picture of the visitor will also be taken. Press Release, Dep't of Homeland Security, US-VISIT Fact Sheet (Oct. 28, 2003).

US-VISIT will also include the interfacing and integration of over twenty existing systems. One of the existing systems that is to be included in the initial implementation of US-VISIT is the Student Exchange Visitor Information System ("SEVIS"), a system that contains information on foreign students in the United States. GAO Homeland Security Report, footnote 1; Appendix I, 32-32.

Data elements of the US-VISIT system include the information made available through arrival and departure manifests. This information includes complete name, date of birth, citizenship, sex, passport number and country of issuance, country of residence, United States visa number, date, place of issuance (where applicable), alien registration number (where applicable), address while in the United States, and such other information that the Attorney General, in consultations with the Secretaries of State and Treasury, determines necessary for the enforcement of the immigration laws and to protect safety and national security. 8 U.S.C. § 1221(c).

The US-VISIT system relies on information provided by visitors traveling to the United States on visas, as opposed to those travelers coming to United States on the Visa Waiver Program ("VWP"). *See* Visa Waiver Permanent Program Act, Pub. L. No. 106-396, 114 Stat. 1637 (2000) (codified as amended at 8 U.S.C. § 1187 (2002)). However, by October 26, 2004, countries in the VWP are required by the USA PATRIOT Act to certify that they will issue their nationals machine-readable passports that incorporate biometric identifiers that comply with the standards established by the International Civil Aviation Organization. Dep't of Homeland Security, *Q&As: Visa Waiver Countries*, footnote 6.

The DHS has stated that the US-VISIT information is to be made available "only to authorized officials and selected law enforcement agencies responsible for ensuring the safety and security of U.S. citizens and foreign visitors." Press Release, Dep't of Homeland Security, DHS Unveils Technology for US-VISIT Entry and Exit Procedures (Oct. 28, 2003).[28] According to DHS, US-VISIT will be available to U.S. Customs and Border Protection Officers at POEs, special agents in the United States Immigration and Customs Enforcement, adjudications staff at U.S. Citizens Immigration Services offices, United States consular offices, and "appropriate federal, state, and local law enforcement personnel." Dep't of Homeland Security, *Q&As: Information Collection & Use* at 3, footnote 6.

However, the USA PATRIOT Act mandates that US-VISIT be able to interface with law enforcement databases to be used by federal law enforcement to identify and detain

---

[28] *Available at* http://www.useu.be/Categories/Justice%20and%20Home%20Affairs/Oct2803USVISIT.html (last visited Nov. 24, 2003).

individuals who pose a threat to national security. 8 U.S.C. § 1635a note. The USA PATRIOT Act also requires that US-VISIT be accessible to all law enforcement and intelligence officers responsible for investigation and identification of aliens. 8 U.S.C. § 1379(3)(C). Under the Aviation and Transportation Security Act, the transmission of manifest information may be shared with other federal agencies, upon request, for the purposes of protecting national security. Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 272 (2001) (codified as amended at 49 U.S.C. § 44909 (c)(2)(F)(5) (2001)).

Moreover, the Data Management Improvement Act of 2000 grants the Attorney General discretion to permit other federal, state, and local law enforcement officials to have access to the data contained in the integrated entry and exit data system for law enforcement purposes. 8 U.S.C. § 1635a(f)(2).

B. Missing Privacy Impact Assessment

The E-Government Act of 2002 requires federal agencies to conduct and publish privacy impact assessments (PIAs) before developing or procuring information technology that will collect or store personal information electronically. Electronic Government Act of 2002, Pub. L. No. 107-347, Title II, 116 Stat. 2910 sec. 208 (2002) (codified as amended at 44 U.S.C. § 3601 note (2003)). However, the DHS has failed to complete the PIA for the US-VISIT program. In the fiscal year 2002 report on expenditure planning for US-VISIT, the GAO made recommendations to the DHS regarding the need to develop this privacy impact assessment and a system security plan. General Accounting Office, *Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning*, GAO-03-563 (June 9, 2003). In fiscal year 2003 expenditure plans, the

GAO reported that the DHS has not yet implemented these recommendations. *See* Press Release, Senate Committee on Governmental Affairs, DHS Violates Privacy Impact Requirements with US VISIT Technology (Dec. 4, 2003).[29]

C. Dramatic Expansion of US-VISIT

After unveiling US-VISIT on October 28, 2003, the DHS now plans to implement US-VISIT at United States air and seaports starting January 5, 2004. US-VISIT will be placed at 115 airports and 14 major seaports by early 2004. Land borders will be phased into US-VISIT throughout 2005 and 2006. International Information Programs Press Release, U.S. Dep't of State, *New Entry-Exit System for Visitors to U.S. Will Be Fast and Effective* (Oct. 28, 2003).[30] The US-VISIT program received $380 million for fiscal year 2003 and has been appropriated $330 million for fiscal year 2004. Press Release, Dep't of Homeland Security, US-VISIT Fact Sheet (2003), footnote 12.

Coordinated efforts, embodied in several pieces of legislation, to enhance immigration procedures and to develop and implement an integrated entry and exit program at all points of entry in the United States is about to become a reality. US-VISIT will integrate data from a variety of data systems and add biometric identifiers of all visitors to the system, but the scope of use of the information within this collective system is still not clear. Thus far, the DHS has failed to complete a privacy impact assessment. The Attorney General possesses broad discretionary powers to allow law enforcement access to this record system.The expansive

---

[29] *Available at* http://www.senate.gov/~gov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=599&Month=12&Year=2003 (last visited Dec. 12, 2003).

[30] *Available at* http://usinfo.state.gov/topical/pol/terror/texts/03102807.htm (last visited Nov. 24, 2003).

purpose of "investigative and identification" leaves open serious questions as to whether US-VISIT, a border control system, will be used routinely on the streets of the America.

CONCLUSION

The technology of government databases has changed dramatically since the Court held in 1968 that police may detain a person and conduct an investigatory stop with less than probable cause. Today, the police have within their electronic reach access to an extraordinary range of government databases. Moreover, every interaction with the police now raises the possibility that a more extensive personal profile will be established, regardless of whether any criminal conduct has occurred.

In recognition of the extraordinary consequences that may flow from police access to government databases, the Court should make clear that the failure to provide personal identification absent probable cause cannot provide the basis for an arrest. In the twenty-first century, significant Constitutional interests are implicated when the government compels the disclosure of personal identification.

Respectfully submitted,

MARC ROTENBERG
Counsel of Record
DAVID L. SOBEL
MARCIA HOFMANN
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009
(202) 483-1140